SERVICE DESCRIPTION
FORTICLOUD

PUBLISHED 8th JUNE 2017

VERSION: 1.2

Contents

SERVICE DESCRIPTION
FORTICLOUD

1. Introduction

FortiCloud is a hosted security, wireless infrastructure management solution and log retention service for FortiGate, FortiWifi and FortiAP devices. Providing solutions for centralized reporting, traffic analysis, configuration management and log retention without the need for additional hardware, software or management overhead.

Through a web based portal a number of benefits can be achieved including:

- Simple provisioning of large scale security and wireless networks.
- Configuration and device management.
- Hosted log retention with cloud based storage.
- Wireless health visibility.
- Rogue access point detection.
- Security inteligence and analytics with FortiView.
- Ad hoc and scheduled reporting.

The service provides a consistent set of features for all supported supported technology, with further specific functionality provided, based on the product type.

2. Service Features & Deliverables

FortiCloud is managed on a twenty-four hours a day by seven days a week basis. It is monitored for hardware availability, service capacity and network resource utilization. The service is made available in various regional SSAE 16 compliant datacenters enabling customers to keep their data within defined boundaries. The service does not share any customer logs or configurations between regional instances.

Through subscribing to the service the following features are included for all supported technolgy:

- Target portal availability of 99.99%.
- Traffic and application visibility through a dashboard view displaying various system and log widgets with real-time monitors.
- FortiView log viewer displaying near real-time activity with ability to filter and download.
- Device management with configuration backup and history, script management and alert profiles.
- Customized reporting with ad-hoc generation and scheduling capability.
- Retention of log files for one year (three hundred and sixty five days) with customization available to reduce unwanted entries.

FortiAP product features include:

- Wireless health monitoring covering bandwidth, usage, clients, interference, failed login and rogue access points.
- Configuration of wireless functionality including SSIDs, authentication, captive portal, platform profiles, tags and network settings.
- Guest management and notification of credentials via email or SMS.
- Social media account integration: ability to connect to wireless accounts via social media.

For Service Providers or MSSPs a multi-tenancy environment can be created through additional subscription, providing:

- Ability to create and manage multiple sub accounts allowing devices to be moved between them.
- Each sub account can be allocated users with access only to their own devices within their own account.

3. Customer Required Contribution & Responsibilities

- Devices must be registered in the Support Portal.
- Configure devices appropriately for use of the FortiCloud service.
- Provide network connectivity with required configuration to enable the devices to communicate with the service. Logs are sent periodically during which time internet connectivity must be available.
- Access the portal through supported web browser software with appropriate internet connectivity.
- Service renewal must be completed before expiration of current term otherwise log files will be purged after 7 days with no grace period.
- Ensure product and FortiOS versions are appropriate to be able to use the service.
- Manage device configuration to ensure any data transmitted is done so in accordance with customer data privary requirements.

The effectiveness of FortiCloud Services is dependant on the configuration utilized by the customer on their local platform and the available bandwidth for communicating the data.

4. Scope and Conditions

- In the event that continued provision of the service to the customer would compromise the integrity or security of the service, the customer agrees that Fortinet may temporarily limit or suspend the Service to the customer.
- Customer agrees to use the service for legitimate and lawful business purposes only. Should Fortinet discover illegal activity, or activity likely to undermine the integrity of the service, regardless of intent, the service may be terminated without notice and where appropriate the relevant authorities notified.
- After the retention period all logs will be deleted permanently.
- Any loss of connectivity by the customer, that is not as a result of failure of Fortinet managed infrastructure, is the responsibility of the customer with the service continuing to be considered as being utilized. Availability targets only apply to the FortiCloud infrastructure.
- Where maintenance of the Fortinet infrastructure is required then Fortinet will aim to perform such maintenance without any service disruption. With any planned maintenance activity that may cause service disruption, Fortinet will provide the customer with forty eight hours advanced notice. Planned maintenance will not be performed between the hours of 8am and 6pm in the time zone where the infrastructure is located, and will not be more than eight hours in any calendar month. Notification will be made through the most appropriate method dependant on user impacted and which may include email, portal messages or other means.
- On the rare occasion that the integrity of the cloud service is at risk then Fortinet may be required to perform emergency maintenance actions. In this instance Fortinet will target to inform all affected parties within one hour of the start of the maintenance activity.
- The service will be delivered in accordance with Fortinet's privacy policy made available and updated from time to time at https://www.fortinet.com/corporate/about-us/privacy.html. The customer is responsible for ensuring that their use of FortiCloud services is in accordance with such laws or regulations.
- The service is available in English or Japanese.

5. Eligibility & Purchasing

The service is available for purchase by an end user through authorized Fortinet resellers and distributors globally. The service is delivered to the customer or end-user of Fortinet products as referenced in the purchase order placed with Fortinet by a customer or Fortinet authorized partner or distributor.

FortiCloud can be ordered in the following format:

Unit	Options	SKU
FortiCloud Log Retention Service (FortiGate/FortiWifi)	*Analysis and 1 Year Log Retention.*	FC-10-00*XXX*-131-02-12
FortiCloud FAP Enterprise Management License	*Includes 1 Year Log Retention and 8x5 FortiCare*	FC-10-90AP1-170-02-DD
FortiCloud FAP-S Enterprise Management License	*Includes 1 Year Log Retention and 8x5 FortiCare*	FC-10-90APS-170-02-DD
FortiCloud – Multi Tenancy License	*Multi Tenancy service for sub accounts.*	FCLE-10-FCLD0-161-02-12

Where *XXX* is defined by the appliance or platform it may apply to. Please refer to your price list to identify the specific SKU for the appropriate Product.

The duration of the service is three hundred and sixty five days from activation of the service. The service may be cancelled by the end-user at any time and for any reason, but in no event will Fortinet refund any prepaid subscription fee. All sales are final.